Attorney's Docket No. 1032326-000132

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Christophe Clavier et al.	Group Art Unit: 2131
Application No.: 09/807,607	Examiner: Kaveh Abrishamkar
Filed: June 1, 2001	Appeal No.: _____
For: COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT USING A SECRET KEY CRYPTOGRAPHIC ALGORITHM	

APPEAL BRIEF

Mail Stop APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the final Office Action dated August 28, 2006, rejecting claims 1-10 and 13-16, which are reproduced in the Claims Appendix of this Brief.

Charge the fee of $500 to Credit Card. Form PTO-2038 is attached.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§1.17 and 41.20 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

06/29/2007 MBELETE1 00000084 09807607
02 FC:1402 500.00 OP

Table of Contents

I. Real Party in Interest

The present application is assigned to Gemplus, a French corporation.

II. Related Appeals and Interferences

There are no other appeals, interferences or judicial proceedings which will affect or be directly affected by, or have a bearing on, the Board's decision in the pending appeal.

III. Status of Claims

The application contains claims 1-16. Claims 11 and 12 have been canceled. Claims 1-10 and 13-16 are pending and stand finally rejected.

This appeal is directed to all rejected claims.

IV. Status of Amendments

There were no amendments filed subsequent to the final Office Action.

V. Summary of Claimed Subject Matter

The claims are directed to countermeasures against external attacks that monitor cryptographic operations for the purpose of discovering secret information, such as keys that are used during the operations. An exemplary embodiment of the countermeasure is described with reference to the DES cryptographic algorithm. This algorithm comprises 16 computation rounds, which are respectively depicted in Figures 7-8 by the labels T1-T16.

The countermeasure method includes the step of executing a first set of instructions in a cryptographic algorithm with a first manipulating means to deliver output data on the basis of input data. Referring to Figure 7, an example of this step is depicted in computation round T2, where the SBOX operation is executed with a first manipulating means that is implemented with a constants table TC_0. An example of such a table is illustrated in Figure 6. The table receives an input signal E1, comprising six bits b1...b6, and produces an output signal S1 having four bits a1...a4.

The method includes the further step of executing another set of instructions with other manipulating means that are derived from the first manipulating means by complementation of at least one of the input data and the output data. Referring again to Figure 7, during computation round T1, the SBOX operation is carried out with the constants table TC_1. An example of this table is illustrated in Figure 9. As can be seen, the output values a1...a4 in this table are the complements of the output values that are delivered by the table TC_0.

The application contains two independent claims, namely claims 1 and 13. A mapping of those claims to representative portions of the disclosure is set forth in the following table:

1. A countermeasure method against attacks by differential analysis of current consumption in an electronic component using a cryptographic algorithm having a secret key, comprising the following steps:	Page 1, lines 3-9
executing a first set of instructions in the algorithm that are critical to said attacks with a first manipulating means to deliver output data on the basis of input data, and	Critical instructions are those that manipulate a target bit (page 7, lines 26-30); this includes the output data of SBOX operations (page 16, lines 12-14 and 21-25); The manipulating means comprises the constants tables TC (page 17, lines 11-15), illustrated in Figures 5, 6, 9 and 10; An example of a first set of instructions is round T2 of the DES algorithm which employs the table TC_0 for the SBOX operation (Figure 7; page 18, lines 1-7)
executing another set of said critical instructions with other manipulating means that are derived from said first manipulating means by complementation of at least one of said input data and said output data, so that the output data and data derived from said output data are unpredictable.	An example of the other manipulating means is the table TC_1 illustrated in Figure 9 (page 17, lines 26-30; page 18, line 20 to page 19, line 3); An example of the other set of critical instructions is round T1 that employs table TC_1 (Figure 7; page 18, lines 8-10); Page 17, lines 15-21
13. An electronic component which provides countermeasures against attacks on a secret key cryptographic algorithm, comprising:	Page 1, lines 3-9; Page 25, lines 15-26; Figure 12

a program memory having stored therein a plurality of different manipulating means for producing output data in response to input data;	Figure 12, program memory 2; page 25, lines 19-22; Manipulating means are tables of constants TC_n, page 17, lines 11-14
a processor which executes instructions in said algorithm that are critical to said attacks, in accordance with a selected one of said manipulating means; and	Figure 12, processor μP executes instructions that manipulate data; page 2, lines 19-23
means for generating a random value for selecting the manipulating means to be employed during a given execution of said algorithm, such that output data produced thereby is unpredictable.	Figure 12, random number generator 4 generates RND1; page 25, lines 22-25; The value of RND1 determines which sequence of tables TC_n will be employed during execution of the algorithm (page 22, line 31 to page 23, line 20)

VI. Grounds of Rejection to be Reviewed on Appeal

The final Office Action presents a single ground of rejection for review on this appeal. Claims 1-10 and 13-16 stand rejected under 35 U.S.C. § 103 on the basis of the Kocher et al patent (US 6,278,783) in view of the Chow et al patent (US 6,594,761).

VII. Argument

A. The Prior Art

The Kocher patent, like the present invention, is concerned with an attacker's ability to derive secure information by observing a series of operations performed in a cryptographic system. However, the approach that is employed by the Kocher patent is different from the present invention. The Kocher patent discloses a technique wherein the message to be encrypted, and/or the encryption keys, are disguised, or "blinded," prior to processing by the DES algorithm. The blinding is accomplished by generating two values which, when combined with one another by means of an Exclusive-OR operation, result in the original message. Permutations of these values are employed to perform the encryption.

The Chow patent discloses a technique for making a computer program resistant to tampering and reverse engineering. In relevant part, it discloses Bit-

Exploded and Bit-Tabulated coding techniques that can be employed to hide data encryption standard (DES) keys. See, for example, column 20, lines 28-29. Beginning at column 20, line 54, the patent discloses a technique in which the entire DES routine is encoded, and then optimized. As set forth at column 21, lines 9-11, "A completely different set of S-boxes has now been produced which bears no discoverable relation to the original ones and correspond only to the encoded data." Thus, the Chow patent discloses replacing the original S-boxes of the DES algorithm with a new set of encoded boxes.

B. Claim 1

Claim 1 recites a countermeasure method that includes the step of executing a first set of instructions in a cryptographic algorithm with a first manipulating means to deliver output data on the basis of input data. The claim recites the further step of executing another set of instructions "with other manipulating means that are derived from said first manipulating means by complementation of at least one of said input data and said output data."

In rejecting claim 1, the Office Action asserts that the Kocher patent discloses the step of executing a first set of instructions in an algorithm with a first manipulating means to deliver output data on the basis of input data, with reference to Figures 1 and 2, and column 1, line 66 to column 2, line 24. The Office Action further asserts that the Kocher patent discloses the step of executing another set of instructions with other manipulating means that are derived from the first manipulating means. Again, reference is made to Figures 1 and 2, as well as column 1, line 66 to column 2, line 24.

In their initial response to this ground of rejection, the Appellants pointed out that it is not apparent from the general reference to Figures 1 and 2, and the cited passage, how the Kocher patent can be interpreted to disclose the claimed subject matter. The Office Action does not explain what is considered to be the first set of instructions, and what is considered to be the other set of instructions. Nor it is apparent what the Office Action considers to be the first manipulating means, or the other manipulating means *that is derived from* the first manipulating means.

In reply to the Appellants' comments, the final Office Action states that the initial permutations illustrated in Figure 1 of the Kocher patent are being interpreted as the claimed first manipulating means, and the other manipulating means are the subkeys. Even with this statement, the record is still unclear as to how the disclosure of the Kocher patent is being correlated with the recitations of the claim. On one hand, the Examiner appears to be stating that the permutation operations constitute the manipulating means. However, the Kocher patent does not discloses that a permutation operation that is performed during step 145, for example, is derived from the permutation operation that is performed at step 120. It does not disclose whether the same permutation, i.e. re-ordering of bits, or a different permutation occurs. Thus, it is unclear whether the same "manipulation means" or different respective manipulation means are employed during the different steps. Even if it is assumed that different permutations are employed, for the sake of argument, there is no disclosure that one of the permutations is "derived from" the other.

On the other hand, the Examiner might be relying upon the keys, per se, as being the manipulating means, since the subkeys are derived from the initial key. In that case, it is not clear how a *key* can be considered to be a manipulating means of the type recited in the claim, i.e. one that delivers output data on the basis of input data. A key does not have input data or output data associated with it. It is simply a string of bits. There is no "manipulating" of data that occurs in a key.

Thus, the Office Action does not establish that the Kocher patent discloses or suggests the claimed steps of executing first and second sets of instructions with respective manipulating means, where one manipulating means is derived from the other.

Claim 1 recites that the derivation of the other manipulating means from the first manipulating means occurs "by complementation of at least one of said input data and said output data." The Office Action acknowledges that one manipulating means of the Kocher patent (however it is being interpreted) is not derived from another manipulating means through complementation of input or output data. To

this end, therefore, it refers to the Chow patent, particularly at column 18, line 50 to column 19, line 13, as well as column 20, line 28.

The Chow patent is concerned with prevention of a user's ability to modify computer software to override built-in controls (column 3, lines 13-16). To accomplish this objective, the patent discloses a technique for *recoding* software, so that it is fragile to tampering (column 5, lines 8-9, and column 9, lines 12-14). Recoding is accomplished by mapping each variable in the software to a new set of variables that cannot be easily traced back to the original variables. (Column 11, lines 8-11). The patent discloses that this technique is also useful for hiding DES keys (column 20, lines 28-29). This portion of the patent goes on to explain one example in which two of the disclosed techniques for hiding variables, namely Bit-Exploded and Bit-Tabulated coding, are employed to hide the DES key. As stated in step 2 at column 21, lines 4-5, when this technique is employed "the key has now completely disappeared".

The Office Action does not establish how the teachings of the Chow patent could be applied to the cryptographic process of the Kocher patent in a manner that would result in the subject matter of claim 1. The claim recites that a first set of instructions are executed with a first manipulating means, and the second set of instructions are executed with other manipulating means "that are derived from said first manipulating means by complementation of at least one of said input data and said output data." As noted above, the Office Action does not identify what is considered to the input data and output data of the Kocher patent that is used to derive one manipulating means from another. Furthermore, there is no disclosure in the Chow patent which suggests that one of the input data or output data associated with one manipulating means, that is employed during the execution of the first set of instructions, can be complemented to derive another manipulating means that is employed during execution of a second set of instructions. To the extent that the Chow patent discloses complementation, it is only for the purpose of *hiding* one set of data, by replacing it with another set of data. There is no disclosure that a complementation function should be employed to derive two different types of

manipulating means that are respectively employed during the execution of different sets of instructions.

As noted previously, the Chow patent discloses the concept *replacing* the original S-boxes of the DES algorithm with a new set of encoded boxes. A reasonable application of this teaching to the system of the Kocher patent would not result in the subject matter of claim 1. There is no suggestion to execute one set of instructions using a first manipulating means, e.g. S-boxes, and to execute another set of instructions using a different set of manipulating means that are derived from the first manipulating means. Rather, since the Chow patent teaches the replacement of the original S-boxes with the encoded S-boxes, all of the instructions would be executed with only the encoded set of S-boxes. There is no suggestion to execute *some* instructions with the original S-boxes, and execute *other* instructions with the encoded S-boxes. As set forth in the Chow patent at column 21, lines 9-11, the original S-boxes no longer exist in the encoded routine.

For at least these reasons, therefore, the Kocher and Chow patents do not suggest the subject matter of claim 1, or any of its dependent claims, to a person of ordinary skill in the art, even when these references are considered in conjunction with one another.

C. Claim 13

Claim 13 recites an electronic component that provides countermeasures against attacks. This component has, among other elements, a processor that executes instructions in a cryptographic algorithm, in accordance with a selected one of a plurality of different manipulating means stored in a program memory. The claim further recites "means for generating a random value for selecting the manipulating means to be employed during a given execution of said algorithm". Thus, the random value is used to select one of the plurality of different manipulating means stored in the memory.

The Office Action acknowledges that the Kocher patent does not discloses this claimed feature, and again relies upon the Chow patent. In responding to Applicants' initial argument traversing this rejection, the final Office Action refers to the Chow patent at column 19, lines 60-64. This passage states that "the positions of the bits in the index and the result of the above lookup can be random... so the encoding chosen for the data is not exposed." The Office Action apparently points to this passage because it contains the word "random". However, the randomness that is discussed in this passage does not relate to the selection of different ones of stored manipulating means for a given execution of an algorithm. The randomness of the positions of bits in an index for a lookup table has nothing to do with the claimed subject matter.

The Office Action does not explain how this disclosure leads a person of ordinary skill in the art to the claimed subject matter. For the sake of argument, even if the different subkeys in the Kocher patent are considered to be different manipulating means, there is no disclosure in the Chow patent suggesting that one of the plurality of subkeys is randomly selected for a given round of the DES algorithm.

As explained previously, a logical application of the teaching of the Chow patent to the process of the Kocher patent would be to employ an encrypted version of the DES routine in place of the original version. In such an implementation, the same S-boxes are employed for each execution of the routine. There is no disclosure in either reference, or in their combination, to utilize a random value to select from among a plurality of different manipulating means for each execution of the algorithm.

Accordingly, the Kocher and Chow patents, even when considered in combination, do not suggest the subject matter of claim 13, or its dependent claims.

D. Claims 3-5

Claim 3 recites that the method comprises executing a first sequence and a second sequence, each of which is made up of at least the first three rounds, such that the order in which the sequences are executed is a function of the one-half

probability statistical relationship, with the first sequence using the first manipulating means in each round, and the second sequence using the other manipulating means in at least the first round. This feature is described in the application beginning at page 22, line 31, with reference to the flow chart of Figure 11. In this procedure, two sequences SEQA and SEQB are both executed, and the value of the random number RND1 determines which sequence is executed first.

In rejecting claim 3, the final Office Action refers to the Chow patent at column 18, line 50 to column 19, line 13, with the observation that it discloses "whether to perform an operation or its complement ..., which provides a one-half probability statistical relationship" (emphasis added). This statement does not establish that the reference discloses the subject matter of the claim. It only shows that one operation or the other is performed, where each one might be performed one-half of the time. In contrast, the claim recites that both sequences are executed, and the statistical probability applies to the order in which they are executed. There is no disclosure in the reference regarding the use of a random value to select the order in which two complementary sequences are executed.

For this additional reason, the rejection of claim 3 is not supported by the references. The rejection of claims 4 and 5, which depend from claim 3, is likewise without support

E. Claim 6

Claim 6 is similar to claim 3, in that it recites that the method comprises executing a first sequence and a second sequence, each of which is made up of at least three rounds, such that the order in which the sequences are executed is a function of the one-half probability statistical relationship. Claim 6 is rejected on the same basis as claim 3. For the reasons presented above, the rejection of this claim is not supported by the references

F. Claims 7-9

Claim 7 depends from claim 6, and recites that the other manipulating means (which is derived from the first manipulating means) comprise second manipulating

means and third manipulating means. The rejection of this claim appears to rely upon the Chow patent at column 18, lines 58-64. This passage discloses that the relationship set forth in line 60 can apply to various binary operations, i.e. other operations besides "AND" and "OR". The use of the word "other" in this passage does not teach that a first manipulating means should be used in one sequence, and that two other manipulating means, which are derived from the first manipulating means, should be used in the other sequence.

For this additional reason, the rejection of claim 7 is not supported by the references. The rejection of claims 8 and 9, which depend from claim 7, is likewise not supported.

G. Claims 10 and 14

Claim 10 depends from claim 1, and recites that the manipulating means are tables of constants. In rejecting this claim, the Office Action refers to the Kocher patent at column 7, lines 15-65, which discloses the use of S tables in the implementation of the DES algorithm. In doing so, the rejection fails to recognize that claim 10 is not reciting the use of tables as manipulating means, per se. Rather, it recites that the manipulating means of claim 1 comprise tables of constants. In other words, when viewed in conjunction with claim 1 from which it depends, claim 10 is reciting that a first table of constants is employed during the execution of a first set of instructions, and that an other table of constants, which is derived from the first table of constants by complementation, is employed in the execution of another set of instructions. The Office Action does not establish that the Kocher patent discloses this claimed subject matter.

Further, the Office Action employs inconsistent interpretations of the reference in rejecting claims 1 and 10. As discussed previously, when rejecting claim 1 the Examiner asserted that the manipulating means of the Kocher patent are the permutations and/or the subkeys. In rejecting dependent claim 10, however, he is suggesting that the S tables constitute the manipulating means, and apparently abandoning the interpretation that relies upon the permutations and the subkeys. It is improper for the Examiner to take such inconsistent positions on the interpretation

of the reference in an effort to reject to different claims that are related to one another. It is incumbent upon the Examiner to identify what elements in the reference are considered to be the manipulating means of claim 1, and then show where the reference teaches that those elements are tables of constants. Reliance upon totally disparate elements does not support the rejection of claim 10.

Claim 14 depends from claim 13, and also recites that the manipulating means are tables of constants. For the same reasons as discussed above, the rejection of this claim is not supported by the references.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

(none)

X. Related Proceedings Appendix

(none)

XI. Conclusion

For the reasons presented hereinabove, the rejection of claims 1-10 and 13-16 is not founded in the statute, and should be reversed.

Respectfully submitted,
BUCHANAN INGERSOLL & ROONEY PC

Date June 28, 2007

By: _____
James A. LaBarre
Registration No. 28632

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620

VIII. CLAIMS APPENDIX

The Appealed Claims

1. A countermeasure method against attacks by differential analysis of current consumption in an electronic component using a cryptographic algorithm having a secret key, comprising the following steps:

executing a first set of instructions in the algorithm that are critical to said attacks with a first manipulating means to deliver output data on the basis of input data, and

executing another set of said critical instructions with other manipulating means that are derived from said first manipulating means by complementation of at least one of said input data and said output data, so that the output data and data derived from said output data are unpredictable.

2. A countermeasure method according to claim 1, wherein said first and said other manipulating means are selected for use on the basis of one-half probability statistical relationship.

3. A countermeasure method according to claim 2, wherein said algorithm comprises sixteen computation rounds, and wherein said method comprises executing a first sequence and a second sequence, each of which is made up of at least the first three rounds, such that the order in which the sequences are executed is a function of the one-half probability statistical relationship, with the first sequence using the first manipulating means in each round, and the second sequence using the other manipulating means in at least the first round.

4. A countermeasure method according to claim 3, wherein each of the first and second sequences is made up of the first three rounds.

5. A countermeasure method according to claim 3, wherein said other manipulating means consist of second means such that, for the same input data, the complement of the output data of the first manipulating means is produced as output data.

6. A countermeasure method according to claim 2, wherein said algorithm comprises sixteen computation rounds, and wherein said method comprises executing a first sequence and a second sequence, each of which is made up of at least the last three rounds, such that the order in which the sequences are executed is a function of the one-half probability statistical relationship, with the first sequence using the first manipulating means in each round, and the second sequence using the other manipulating means.

7. A countermeasure method according to claim 6, wherein each of the first and second sequences is made up of the last three rounds, and wherein the other manipulating means used in the second sequence comprise second manipulating means and a third manipulating means.

8. A countermeasure method according to claim 7, wherein said second manipulating means are such that, for the same input data, the complement of the output data of the first manipulating means is produced as output data, and wherein said second manipulating means are used in the second sequence for the fourteenth round.

9. A countermeasure method according to claim 8, wherein said third manipulating means are such that, for the complement of the input data, the complement of the output data of the first manipulating means is produced as output data, and wherein said third manipulating means are used in the second sequence for the fifteenth round and the sixteenth round.

10. A countermeasure method according to claim 1 wherein said manipulating means are tables of constants.

13. An electronic component which provides countermeasures against attacks on a secret key cryptographic algorithm, comprising:

a program memory having stored therein a plurality of different manipulating means for producing output data in response to input data;

a processor which executes instructions in said algorithm that are critical to said attacks, in accordance with a selected one of said manipulating means; and

means for generating a random value for selecting the manipulating means to be employed during a given execution of said algorithm, such that output data produced thereby is unpredictable.

14. The electronic component of claim 13 wherein said manipulating means comprise tables of constants.

15. The electronic component of claim 13 wherein said different manipulating means respectively produce sets of output data that are complementary to one another.

16. The electronic component of claim 13, wherein said component is a smart card.